AO 106 (Rev. 06/09) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of New York

11 MAG 2754

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
PLEASE SEE ATTACHMENT A

Case No.

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:
A hard drive obtained from U.K. law enforcement officials on or about September 15, 2011, containing the forensic copies of computers #1, #2, and #3, currently stored at the NY Field office of the FBI

located in the Southern District of New York, there is now concealed *(identify the person or describe the property to be seized)*:

PLEASE SEE ATTACHMENT B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. Sections 1030 and 371.	Computer intrusion and conspiracy to do same.

The application is based on these facts:

PLEASE SEE AFFIDAVIT AND ATTACHMENT A.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Olivia D. Olson, FBI Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 10/27/2011

Judge's signature

City and state: New York, New York

Printed name and title

THEODORE H. KATZ
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR A SEARCH WARRANT FOR THE PREMISES KNOWN AND DESCRIBED AS A HARD DRIVE, OBTAINED FROM U.K. LAW ENFORCEMENT OFFICIALS ON OR ABOUT SEPTEMBER 15, 2011 IN LONDON, ENGLAND, CONTAINING THE FORENSIC COPIES OF COMPUTERS #1, #2, AND #3, CURRENTLY STORED AT THE NEW YORK FIELD OFFICE OF THE FEDERAL BUREAU OF INVESTIGATION.	**TO BE FILED UNDER SEAL** AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT

OLIVIA D. OLSON, being duly sworn, deposes and says:

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"). I have been an FBI Special Agent since 2009 and have been assigned to the Criminal Cyber Intrusion squad within the New York Division of the FBI since 2010. As part of my work at the FBI, I have received training regarding computer technology, computer fraud, and white collar crimes and in the manner and means by which individuals use computers and the internet to commit such crimes. I have participated in the execution of search warrants involving electronic crimes. From my examination of reports and records and my conversations with other law enforcement agents and other individuals I am familiar with the facts and circumstances set forth below.

2. I make this Affidavit in support of an application for a search warrant for a Hard Drive, obtained from law enforcement officials from the United Kingdom (the "U.K. Law

Enforcement officials") on or about September 15, 2011 in London, England, containing the forensic copies of COMPUTERS #1, #2, and #3, currently stored at the New York Field Office of the Federal Bureau of Investigation (hereinafter the "PREMISES" or TARGET HARD DRIVE). For the reasons detailed below, I believe that there is probable cause to believe that on the TARGET HARD DRIVE there exists evidence, fruits, and instrumentalities of violations of (and conspiracy to commit violations of) Title 18, United States Code, Section 1030 (computer hacking), among other crimes (the "TARGET OFFENSES").

3. Because this Affidavit is being submitted for the limited purpose of establishing probable cause for a warrant to search the PREMISES, I have not included every detail of every aspect of the investigation. Rather, I have set forth only those facts that I believe are necessary to establish probable cause. The information contained in this Affidavit is based upon conversations with other law enforcement officers and others, my review of various documents and records, and, where specified, my personal observations and knowledge. Unless specifically indicated, all conversations and statements described in this Affidavit are related in substance and in part only.

TECHNICAL BACKGROUND

4. As noted above, I have had both training and experience in the investigation of computer-related crimes. Based on my training and experience, I know the following:

a. **The Internet.** The Internet is a worldwide network of computer[1] systems operated by governmental entities, corporations, and universities. In order to access the Internet, an individual computer user must subscribe to an access provider, which operates a host computer system with direct access to the Internet. The world wide web ("www") is a functionality of the Internet which allows users of the Internet to share information. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. This connection can be made by any number of means, including modem, local area network, wireless and numerous other methods.

b. **E-mail.** E-mail is a popular form of transmitting messages and/or files in an electronic environment between computer users. When an individual computer user sends e-mail, it is initiated at the user's computer, transmitted to

---

[1] The term "computer" as used herein is defined in 18 U.S.C. § 1030(e)(1), and includes an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

the subscriber's mail server, then transmitted to its final destination. A server is a computer that is attached to a dedicated network and serves many users. An e-mail server may allow users to post and read messages and to communicate via electronic means.

c. **Internet Service Provider ("ISP").** An ISP is a commercial service that provides Internet connections for its subscribers. In addition to providing access to the Internet via telephone or other telecommunications lines, ISPs may also provide Internet e-mail accounts and other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with them. Those records could include identifying and billing information, account access information in the form of log files, e-mail transaction information, and other information.

d. **IP address.** The Internet Protocol address (IP address) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range of 0-255, separated by periods. Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses.

e. **Server.** A server is a centralized computer that provides services for other computers connected to it via a network or the Internet. The computers that use the server's services are sometimes called "clients." When a user accesses email, Internet web pages, or files stored on the network itself, those files are pulled electronically from the server, where they are stored, and are sent to the client's computer via the network or Internet. Notably, server computers can be physically located in any location; for example, it is not uncommon for a network's server to be located hundreds (or even thousands) of miles away from the client computers. In larger networks, it is common for servers to be dedicated to a single task. For example, a server that is configured so that its sole task is to support a World Wide Web site is known simply as a "Web server." Similarly, a server that only stores and processes e-mail is known as a "mail server."

II. Probable Cause Exists To Search The TARGET HARD DRIVE

5. As noted above, on or about September 15, 2011, I was given the TARGET HARD DRIVE by the U.K. Law Enforcement officials, who are members of the Metropolitan Police ("MET") in London, England. I was told by the U.K. Law Enforcement officials, in substance and in part, that the TARGET HARD DRIVE that constitutes the PREMISES contained forensic copies of three separate computer hard drives (the Three Computers or COMPUTERS

#1, #2, and #3 collectively). The Three Computers were seized by the U.K. Law Enforcement officials pursuant to U.K. law. As set forth below, there is probable cause to believe that the TARGET HARD DRIVE may contain evidence of the TARGET OFFENSES in light of the connection that each of the Three Computers, forensic copies of which are contained on the TARGET HARD DRIVE, has to a suspected sophisticated computer hacker.

6. Based on my familiarity with the investigation, I know that, for the past several months, the FBI has conducted an investigation of several online groups, including "Anonymous" and "LulzSec," that are responsible for multiple cyber attacks on the computer systems of various business and governmental entities in the United States and elsewhere.

7. Based on my familiarity with the investigation, from in or about late 2010 up to and including the present, members of these groups engaged in, among other things, (i) the theft and later the dissemination of confidential information, including the personal identifying information of individuals, from computer systems; (ii) the defacement of Internet websites; and (iii) attacks against websites, known as "distributed denial of service" or "DDoS" attacks, which involved the use of a large number of computers to bombard a victim's website with bogus requests for information, causing the website to temporarily cease to function.

8. Based on my investigation, I have learned that three of the major figures involved in Lulzsec use the on-line monikers "Kayla," "Topiary," and "T-Flow" respectively.

9. In early June 2011, the FBI arrested an individual ("CW-1") on charges of credit card fraud, who, since the time of his/her arrest, has been cooperating with the Government. The information provided by CW-1 has been shown to be reliable and has been corroborated by other evidence. Among other things, CW-1 has informed the FBI that individuals known by the online nicknames "Topiary," "T-Flow" and "Kayla" are members of Anonymous and LulzSec and have participated in the hacking activity of those groups.

10. From the time of his arrest in early June 2011, up to the present, CW-1 has been proactively cooperating with the FBI and engaged in consensually monitored and recorded internet chats with Topiary, Kayla, and T-Flow.[2] I have reviewed these chats and they reveal that CW-1 discusses computer hacking activities with Topiary, Kayla, and T-Flow.

11. T-Flow - Computer #1:

---

[2] Based on my experience investigating computer crimes, I know that it is not unusual for computer hackers to use multiple internet names and email addresses to mask their identities, sometimes within the same internet chat session. Accordingly, in some of the chats recorded with CW-1, both CW-1 and CW-1's correspondents, including Topiary, T-Flow and Kayla, use various and different nicknames. However, CW-1 was aware of the different names used by the others and, in addition, the members of LulzSec had developed a means of verifying each others' identities by use of predetermined codenames.

a. According to CW-1, almost immediately after CW-1 became involved in Anonymous, CW-1 was contacted in an Internet chat room for Anonymous hackers by an individual using the online nickname "T-Flow." T-Flow asked CW-1 certain questions designed to test CW-1's knowledge of computer hacking, and, after being satisfied by CW-1's answers, invited CW-1 to join an elite group of hackers associated with Anonymous that was known as "Internet Feds." Among other things, in or about February 2011, the members of Internet Feds, including CW-1 and T-Flow participated in an attack on the computer servers of HBGary, a cyber security company in the United States, that involved the theft (and later dissemination) of confidential information, including email messages.

b. According to CW-1, in May 2011, some of the members of Internet Feds, including CW-1 and T-Flow, left the group to start a new hacking group, LulzSec. The core members of LulzSec include T-Flow and five other individuals (including CW-1) who use the following online nicknames: Topiary, AVUnit, Sabu, Kayla, and Pwnsauce. According to CW-1, T-Flow's specific role within LulzSec was to act as an organizer and coordinator who helps direct the activities of the group's members. In May 2011 and June 2011, the members of LulzSec participated in many hacks of governmental and business websites, including, among others, Sony Pictures Entertainment; the Public Broadcasting Service;

Nintendo, a video game company based in Japan; the Atlanta chapter of Infragard, an information sharing partnership between the FBI and private industry concerned with protecting critical infrastructure in the United States; Unveillance, a cyber security firm headquartered in Delaware; the United States Senate; and Bethesda Softworks, a video game company based in Maryland.

c. Based on my investigation and conversations with the U.K. Law Enforcement officials, I have learned that COMPUTER #1, one of the three computers forensically copied on the TARGET HARD DRIVE belongs to T-Flow based on the following, in substance and in part:

(i) On or about July 19, 2011, the MET arrested a 16-year-old minor in London named Mustafa Al-Bassam ("Al-Bassam") whom they believed to be the hacker known as "T-Flow." At the time of the arrest, Al-Bassam was interviewed consistent with U.K. legal requirements and admitted to the MET that he was T-Flow and admitted to membership in Lulzsec. (However, when later interviewed by the MET, he refused to sign a written confession that he was Tflow. To date, the MET has not pursued criminal charges against him.)

(ii) The MET conducted a lawful search under U.K. law of Al-Bassam's residence including a jacket in a room used by Al-Bassam. The jacket appeared to match Al-Bassam's size. In

the pocket of that jacket, the MET discovered a sheet of paper with a handwritten chart.

(iii) The chart is entitled "#internetfeds history" and contains details, under specific column headings like "victim" and "other helpers," of cyber attacks against approximately 11 different victims that had been carried out by Internet Feds and/or Lulzsec or were being planned, and included a listing of the hackers involved in each attack. The hacks listed include some hacks known to the FBI which members of Lulzsec are suspected of orchestrating, including of the computer networks of HBGary, the security firm mentioned above. The chart also lists a planned attack on fbi.gov, the website for the FBI, and indicates that T-Flow discovered the vulnerability. In addition, many of the hackers listed are known to the FBI for their involvement in Lulzsec, including Topiary, Kayla, and pwnsauce.

(iv) The MET seized COMPUTER #1 from the Al-Bassam residence. They conducted a preliminary search of COMPUTER #1; however, no forensic evidence of note was discovered. They have requested that the FBI assist them in conducting a search of COMPUTER #1.

12. Topiary - Computer #2

a. Based on my familiarity with the investigation, including information obtained from CW-1 as noted

above, I know that a hacker who uses the online nickname Topiary is a member of Anonymous and LulzSec. The FBI's investigation has revealed that Topiary's role within the groups involved, among other things, (i) acting as a spokesperson for the groups; (ii) defacing websites that were compromised by the groups; and (iii) "socially engineering" victims, that is, tricking the victim, the victim's Internet service provider, or other company into disclosing sensitive information, such as usernames and passwords, that can be used by hackers to gain access to the victim's computer system.

b. I have reviewed chats between CW-1 and Topiary where they discuss hacking activities that they have participated in connected to Lulzsec and Anonymous. In addition, Topiary has also been intercepted in chats with a source used by another FBI office (CW-3) in similar conversations about hacking activities.

c. Based on my investigation and conversations with the U.K. Law Enforcement officials, I have learned that Computer #2, one of the three computers forensically copied on the TARGET HARD DRIVE, belongs to Topiary based on the following:

(i) In or about late June 2011, agents in the FBI's Los Angeles Office ("FBI-LA") obtained a pen register on a Twitter account that was used by multiple members Lulzsec (the "Lulzsec Twitter Account"), including Topiary who, as Lulzsec's spokesperson, was one of the primary users of the Lulzsec Twitter

Account based on the communications on the account. Through the pen register, the FBI obtained IP addresses from which individuals using the Lulzsec Twitter Account were accessing the Internet, including some which belonged to a virtual private network service (VPN)[3] based in the United Kingdom (the "UK VPN Service"). I know, based on my training and experience with cybercrime and computer hacking investigations that the UK VPN Service is a web proxy service that is often used by those engaged in computer hacking activities to access the Internet in a manner that will mask their IP addresses or other information that might identify their location or identity. FBI-LA provided the IP addresses obtained from the Lulzsec Twitter Account, as well as data such as the date and time of access, to the U.K. Law Enforcement officials.

(ii) FBI-LA obtained additional IP addresses from the Lulzsec Twitter Account between in or about July 15, 2011 and July 22, 2011, some of which belonged to the same U.K. VPN Service, and provided those to the U.K. Law Enforcement officials as well. The U.K. VPN Service provided the U.K. Law Enforcement officials with all of the subscriber information related to the various IP addresses that FBI-LA had provided from the Lulzsec Twitter Account pen register. Based on a comparison of the

---

[3] A virtual private network or VPN service provides users a private secure network within a public communications system, such as the Internet.

subscriber information connected to the various IP addresses, the U.K. Law Enforcement officials identified a residence in the Shetland Islands (United Kingdom) belonging to the family of an individual named "Jake Davis" as a location of interest. Topiary had indicated on the Lulzsec Twitter Account that s/he was in the process of moving. Additional investigation revealed another location that was also identified as a residence of "Jake Davis."

(iii) The U.K. Law Enforcement officials conducted searches of the two residences associated with Jake Davis and his family consistent U.K. legal requirements on or about July 27, 2011. They also interviewed Jake Davis consistent with U.K. legal requirements, who admitted, in substance and in part, that he was "Topiary." Among other items, they retrieved COMPUTER #2, which is one of the three Hard Drives on the TARGET HARD DRIVE.

13. Kayla - Computer #3:

a. As noted above, CW-1 has also identified an individual who uses the online nickname "Kayla" as an individual who is an active member of Anonymous and Lulzsec. I have reviewed communications between CW-1 and Kayla in which they discuss hacking activities that they have participated in connected to Lulzsec and Anonymous.

b. In addition, I have learned about Kayla's involvement in hacking activities and Kayla's contact information through the following:

(i) On or about December 11, 2010, according to published reports, computer networks of Gawker Media, an online media company and blog network, were "hacked," or broken into, resulting in the theft of a large amount of information, including a database of over one million usernames and encrypted passwords of individuals who had registered for accounts on a variety of affiliated Gawker websites (the "Gawker Hack"). A group calling itself "Gnosis" claimed responsibility for the attack in public statements in the days following this intrusion.

(ii) On or about June 29, 2011, I participated in the arrest of an individual on a computer hacking related charge pursuant a Criminal Complaint filed in the Southern District of New York ("CW-2"). Following the arrest, CW-2 attempted to cooperate with law enforcement in the hopes of reducing CW-2's sentencing liability. I have found that the information that CW-2 has provided has been generally corroborated by other evidence developed during the course of this investigation.[4] As part of his/her attempted cooperation, CW-2 has been debriefed by the

---

[4] After CW-2 was arrested, at the request of defense counsel, the Government arranged for a court-ordered mental competency evaluation of CW-2. The psychological evaluation indicates that CW-2 has a form of autism, which can affect his/her social interaction and judgment, among other things. However, based on my interactions with CW-2, CW-2 also appears to be highly-functioning in other areas, including the ability to recall information, and the assistance that CW-2 has provided to law enforcement to date has been corroborated by other information and, based on my participation in this investigation, has proven credible.

Government. During those debriefings, CW-2 stated, in substance and in part, that CW-2 was in online contact with an individual using the online nickname "Kayla", who provided CW-2 with the stolen database of over one million usernames and encrypted passwords for Gawker users and tasked CW-2 with decrypting the passwords; and CW-2 communicated intermittently with Kayla over the course of at least the past year.

(iii) I reviewed CW-2's instant messenger contact list with CW-2's consent. Based on my review, I learned that it includes a contact labeled "Kayla." CW-2 confirmed that this is the contact listing for the Kayla with whom CW-2 participated in the Gawker Hack. Clicking on the Kayla contact listing revealed what appeared to be a user profile for that contact, including a personal email account (the "Kayla Email Account"). CW-2 also provided the name under which Kayla communicates on Twitter. Based in part on the information provided by CW-2 the Government obtained a search warrant (11 Mag. 1767) and pen register, 11 Mag. 1782 and 11 Mag. 2376) for the Kayla Email Account and a pen register (11 Mag. 1882) for the Kayla Twitter Account.

c. Based on my investigation and conversations with the U.K. Law Enforcement officials, I have learned that Computer #3, one of the three computers forensically copied on the TARGET HARD DRIVE belongs to Kayla based on the following:

(i) As a general matter, the pen traffic that was obtained for both the Kayla Email Account and the Kayla Twitter Account indicated that they were accessing the internet through numerous different internet protocol addresses around the world. This pattern reflected a common practice by highly-skilled computer hackers of utilizing "proxy" accounts to access the Internet which permit them to mask the internet protocol address and thus the location from which they are accessing the internet, as noted above with regard to the U.K. VPN Service. However, based on my experience in such investigation, I know that occasionally even the most skilled computer user's internet access will at times reflect the same internet protocol address on more than one occasion: because the recurrence of an internet protocol address is unlikely with the use of a proxy, I know from experience that when an IP address recurs in the pen information, it is likely that the target mistakenly accessed the internet without a proxy and thus the recurring IP address is likely to indicate the target's likely location.

(ii) Based on pen traffic obtained for the Kayla Email Account and for the Kayla Twitter Account, I learned that both had accessed the internet through one IP address (the "IP Address") based in the United Kingdom on separate occasions. Specifically the Kayla Email Account accessed the Internet on one occasion in December 2009 and again in March 2011 from that IP

Address, and the Kayla Twitter Account had accessed the Internet on one occasion in June 2011 from that IP Address. Records showed that this IP Address was associated with an internet service provider in Doncaster, in the United Kingdom. I have also learned through reviewing Kayla's communications on the Internet with CW-2 that Kayla used British spellings of words. Accordingly, the information about the IP Address was provided to U.K. law enforcement for further investigation.

(iii) Based on my conversations with the U.K. Law Enforcement officials, I have learned that they obtained the records from the provider for this IP Address which indicated that it was registered to an individual at a residence in Doncaster, United Kingdom. Investigation revealed that the household included parents, two sons, and a daughter. The daughter had a name that was pronounced like "Kayla" in that region of the United Kingdom (although spelled differently). However, the investigators learned that she did not reside at the house. The two sons did, however, along with the parents. Based on physical surveillance and simultaneous monitoring of the Kayla Twitter Account, the U.K. Law Enforcement officials identified the son named Ryan Ackroyd as the individual who was using the Kayla Twitter Account. By coordinating their surveillance with the Twitter Account activity, the investigators conducted a search, consistent with U.K. law, of the residence, and arrested

Ryan Ackroyd, along with his brother. The parents and the brother confirmed that Ryan Ackroyd was highly skilled at computers, which he denied. COMPUTER #3 was seized from Ryan Ackroyd, and U.K. Law Enforcement officials have requested the FBI's

assistance in reviewing the forensic copy they provided via the TARGET HARD DRIVE.

14. Based on my training and experience and knowledge of this investigation, I believe that the TARGET HARD DRIVE likely contain evidence, fruits, and/or instrumentalities of the TARGET OFFENSES. Based on my training and experience, programs, data, files, and other records reflecting computer intrusion related activities are often stored on computers used by individuals involved in those offenses. Hard drives are also often used to store files and data, including defaced pages or other records, for later use by hackers. Hard drives also may contain records of locations, log in times and dates, access, contacts and other information related to communications and internet access related to computer intrusion activities. This can be the case even if individuals involved in the offenses have attempted to clear their hard drives of any such records.

15. Based on the foregoing, there is probable cause to believe that the TARGET HARD DRIVE contains forensic copies of COMPUTERS #1, #2 and #3, seized by U.K. law enforcement and belonging to individuals believed to be the on-line hackers Topiary, T-Flow, and Kayla, and that those hard drives contain evidence of criminal activity related to Anonymous and Lulzsec.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

16. As described above and in Attachment A, this application seeks permission to search and seize records on the PREMISES, the TARGET HARD DRIVE, which contains forensic copies of three computers previously seized by the U.K. law enforcement authorities, and currently stored at the FBI, in whatever form they are found. The PREMISES stores information in electronic or digital format. Some of these electronic records might take the form of files, documents, and other data that is user-generated. Some of these electronic records, as explained below, might take a form that becomes meaningful only upon forensic analysis.

17. I submit that there is probable cause to believe those records will be stored in above described manner, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium such as a computer hard drive,

deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space-that is, in space on the storage medium such as a computer hard drive that is not currently being used by an active file-for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media - in particular, computers' internal hard drives - contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this

information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

18. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for evidence that establishes how computers were used, the purpose of their use, who used them, and when.

19. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processor, picture, and movie files), computer storage media can contain other forms of electronic evidence as well:

a. Forensic evidence of how computers were used, the purpose of their use, who used them, and when, is, as described further in Attachment B, called for by this warrant. Data on the storage medium not currently associated with any file can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted

portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, and correspondence (and the data associated with the foregoing, such as file creation and last accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence

in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance with particularity a description of the records to be sought, evidence of this type often is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand the evidence described in Attachment B also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, I know from training and experience that it is possible that malicious software can be installed on a computer, often without the computer user's knowledge, that can allow the computer to be used by others, sometimes without the knowledge of the computer owner. Also, the presence or absence of counter-forensic programs (and

associated data) that are designed to eliminate data may be relevant to establishing the user's intent. To investigate the crimes described in this warrant, it might be necessary to investigate whether any such malicious software is present, and, if so, whether the presence of that malicious software might explain the presence of other things found on the storage medium. I mention the possible existence of malicious software as a theoretical possibility, only; I will not know, until a forensic analysis is conducted, whether malicious software is present in this case.

20. Searching storage media such as a computer hard drive for the evidence described in the attachments may require a range of data analysis techniques. It is possible that the storage media located on the premises will contain files and information that are not called for by the warrant. In rare cases, when circumstances permit, it is possible to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. For example, it is possible, though rare, for a storage medium to be organized in a way where the location of all things called for by the warrant are immediately apparent. In most cases, however, such techniques may not yield the evidence described in the warrant. For example, information regarding user attribution or

Internet use is located in various operating system log files that are not easily located or reviewed.

21. As explained above, because the warrant calls for records of how a computer or storage media has been used, what it has been used for, and who has used it, it is exceedingly likely that it will be necessary to thoroughly search storage media to obtain evidence, including evidence that is not neatly organized into files or documents. Just as a search of a premises for physical objects requires searching the entire premises for those objects that are described by a warrant, a search of this premises for the things described in this warrant will likely require a search among the data stored in storage media for the things (including electronic data) called for by this warrant. Additionally, it is possible that files have been deleted or edited, but that remnants of older versions are in unallocated space or slack space. This, too, makes it exceedingly likely that in this case it will be necessary to use more thorough techniques.

22. Based upon my knowledge, training and experience, I know that a thorough search for information stored in storage media such as a computer hard drive often requires agents to seize most or all storage media to be searched later in a controlled environment. As described above, the computers described in this warrant have already been lawfully seized

incident to arrest by foreign law enforcement. This Offsite search of storage media is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. Additionally, to properly examine the storage media in a controlled environment, it is often necessary that some computer equipment, peripherals, instructions, and software be seized and examined in the controlled environment. This is true because of the following:

(i) The nature of evidence. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable.

(ii) The volume of evidence. Storage media can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to peruse all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search

on-site.

(iii) Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on-site. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

(iv) Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

CONCLUSION

23. Based upon the information above, I submit that there is probable cause to believe that concealed within the previously-seized TARGET HARD DRIVE currently stored at the FBI,

there exists evidence, fruits, and instrumentalities set forth with particularity in Attachment A, relating to violations of the TARGET OFFENSES.

OLIVIA D. OLSON
Special Agent
Federal Bureau of Investigations

OCT 27 2011

Subscribed and sworn before me
this __ day of October, 2011.

HONORABLE ~~KEVIN NATHANIEL~~ FOX
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK

THEODORE H. KATZ
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK

ATTACHMENT A

Premises to be searched:

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR A SEARCH WARRANT FOR THE PREMISES KNOWN AND DESCRIBED AS A HARD DRIVE, OBTAINED FROM U.K. LAW ENFORCEMENT OFFICIALS ON OR ABOUT SEPTEMBER 15, 2011 IN LONDON, ENGLAND, CONTAINING THE FORENSIC COPIES OF COMPUTERS #1, #2, AND #3, CURRENTLY STORED AT THE NEW YORK FIELD OFFICE OF THE FEDERAL BUREAU OF INVESTIGATION.

ATTACHMENT B

Items to be searched for and seized:

1. All records relating to violations of the statutes listed on the warrant and involving Anonymous, Lulzsec, Gnosis, any of the computer hacks associated with these groups, CW-1, CW-2, Topiary, TFlow, or Kayla, or any of their associates, including any and all notes, documents, records or correspondence in any format and medium pertaining to computer intrusion or hacking activities. Any records of correspondences in relation to the possession, trafficking or distribution of any of information obtained through computer intrusion activities.

2. For each COMPUTER contained on the TARGET HARD DRIVE:

A. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

B. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

C. evidence of the lack of such malicious software;

D. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

E. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

F. evidence of the times the COMPUTER was used;

G. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

H. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER; and

I. contextual information necessary to understand the evidence described in this attachment.